Before the
Federal Communications Commission
Washington, DC 20554

In the matter of	)	
	)	
Reliability and Continuity of Communications Networks, Including Broadband Technologies	)	PS Docket no. 11-60
	)	
Effects on Broadband Communications Networks Of Damage or Failure of Network Equipment of Severe Overload	)	PS Docket No. 10-92
	)	
Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks	)	EB Docket No. 06-119

Comments by Rural Broadband, LLC

Rural Broadband, LLC respectfully submits the following reply comments in response to the *Notice of Inquiry* adopted by the Commission on April 7th, 2011, and the public comments filed in the consolidated proceedings.

Rural Broadband, LLC is a team of broadband industry professionals with over 150 years of combined experience at developing and operating broadband delivery networks both wired and wireless. Rural Broadband team members have been involved in the design, deployment and integration of wireless broadband networks for public safety for over ten years and have been closely involved in nationwide 4G wireless projects in the United States.

On August 2, 2010 Rural Broadband, LLC filed a 700 MHz PS Waiver Petition on behalf of four jurisdictions in GA as the Georgia Broadband Alliance and we continue to advise multiple municipalities on the development and capitalization of Public Safety Broadband Networks. Rural Broadband, LLC is a member of the Verizon LTE Developers Conference and the PCSR Public Safety Network Demonstration Team.

Chapter 16 of the National Broadband Plan laid out a vision of a National Broadband Network for Public Safety that would be leveraged off of the cellular carrier's nationwide deployment of 4G services. The National Broadband Plan recognized that colocation on existing commercial facilities would be essential in order to achieve the 97% nationwide coverage specified.

Section 16-B of the National Broadband Plan calls for:

- Construction of a public safety 700 MHz broadband network that involves partnerships and uses commercial infrastructure, the public safety infrastructure or both through incentive-based partnerships.

- Hardening of the existing commercial network and new sites that operate as part of the public safety network

In section 16.12 of the National Broadband Plan, it recommends that the "FCC explore broadband communications reliability and resiliency". In reviewing earlier comments from cellular carriers and after attending FCC and PCSR hosted meetings regarding Network Resiliency and Reliability, we have found the discussions primarily focused on the cybersecurity of the network and the need for backup power at the cell site. While we agree that these topics are essential to the survivability of the public safety network, we would like to take this opportunity to raise another issue relative to network resiliency which we feel has been given insufficient consideration to this point, physical security of the cell sites.

Cell sites regularly experience break-ins for theft of copper ground wires, grounding bars and coax cable, items with a salvage value of a few hundred dollars but the resultant damage can cost the

carriers and tower owners many thousands to mitigate. Unfortunately, these break-ins (at best) leave the site vulnerable and can often result in taking the site completely out of service.

According to a 2008 FBI report, Copper theft represents a clear and present threat to our nation's critical infrastructure. The report states that "China, India, and other developing nations are driving the demand for raw materials such as copper and creating a robust international trade. Copper thieves are receiving cash from recyclers who often fill orders for commercial scrap dealers. Recycled copper flows from these dealers to smelters, mills, foundries, ingot makers, powder plants, and other industries to be re-used in the United States or for supplying the international raw materials demand. As the global supply of copper continues to tighten, the market for illicit copper will likely increase". The FBI is at this time writing an update to this report to reflect the recent increase in copper theft.

Commodity prices for copper have risen from $.60 per pound in 2002 to more than $4.00 per pound in August of 2011. Consequently, the theft of copper from telephone lines, electrical substations, highway infrastructure, residential homes and cell towers has grown exponentially. Cell sites make easy targets because they are often located in places that are not visible to the public and contain large amounts of easily accessible copper.

The issue is complicated by the fact that cell towers are often owned by third parties who lease space on the towers to multiple carriers. The question arises; "whose responsibility is it to secure the tower"? The tower owner can provide chained locks and provide the carriers with keys or combinations but this means that all the carriers, their engineering/maintenance personnel and contractors must have access. Keys and combinations can be copied and passed around. The absence of access control systems at cell sites means that any group of people with a pickup and hardhats could pass themselves off as contractors with a legitimate reason to be on the property.

There is a variety of electronic surveillance systems specifically developed to address cell site security including access control systems, video surveillance and intrusion detection. Unfortunately, to this point the tower owners and carriers have balked at the costs of the hardware, monitoring and the required communication bandwidth.

We feel that this vulnerability needs to be assessed further and suggest developing physical security guidelines similar to the ones written and enforced by NERC (North American Reliability Council) to provide guidance to the operators of the nation's electrical grid on how to provide physical security to the bulk electric system. NERC IV CIP 006 details the steps that should be taken to control access to "Critical Access Points" within the electrical system, perhaps some consideration should be given to developing a similar set of standards for physical security of all cell sites used in the National Broadband Network for Public Safety.

In conclusion, cell site break-ins, whether for vandalism, copper theft or more nefarious reasons are topics which should be given ample consideration in the discussion of network reliability and resiliency. We believe the FCC should propose security standards that would proscribe to tower owners the steps that should be taken to minimize unauthorized entry for all cell sites involved in the National Broadband Public Safety network.

dhimes@ruralbroadbandllc.com